IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

JOHN CARMACK, and all others similarly situated, Plaintiff, vs. SNAP-ON, INC., Defendant.	**Case No. 22-cv-695**

CLASS ACTION COMPLAINT

Plaintiff John Carmack, ("Plaintiff" or "Mr. Cormack"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Snap-On, Inc. ("Defendant" or "Snap-On"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

NATURE OF THE CASE

1. Plaintiff brings this class action against Defendant for its failure to exercise reasonable care in securing and safeguarding individuals' sensitive personal data on a massive scale.

2. Defendant first learned that an unauthorized party had gained access to its computer network on March 1, 2022.[1] Between March 1 and March 3, 2022, a malicious third

[1] On information and belief, the attack on Snap-On's systems was perpetrated by the infamous Conti ransomware gang, which is a known cybercrime organization that targets individuals' information on companies' systems and sells it specifically for the purpose of stealing consumer information and effectuating identity theft. It is therefore indisputable that the ransomware attack was a targeted attempt to steal Snap-On employees' information and use it for illegal purposes. *See* Lawrence Abrams, *Snap-On discloses data breach claimed by Conti ransomware gang*, BLEEPINGCOMPUTER, https://www.bleepingcomputer.com/news/security/snap-on-discloses-data-breach-claimed-by-conti-ransomware-gang/ (last visited June 9, 2022).

party accessed and exfiltrated files and data stored on Defendant's computer systems (the "Data Breach"). The stolen data included names, Social Security numbers, dates of birth, and employee identification numbers ("Private Information").

3. On or around April 7, 2022, Defendant announced that the Data Breach involved sensitive employee data.[2] On or around this date Defendant sent the first notice of the Data Breach to some of those impacted, including Plaintiff.

4. Defendant manufactures American automotive tools nationwide.[3] Defendant has global reach, with 12,800 employees worldwide, $4.25 billion in revenue in 2021, and reach in 130 countries. In the U.S. alone, Snap-On has 3,400 franchise vans and 13 manufacturing facilities. By storing the sensitive information of thousands of its employees, Defendant had a heightened duty to protect Plaintiff and other Class members' Private Information.

5. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiff and other members of the Class (as defined below). These failures compromised Plaintiff and other Class members' Private Information and placed them at a serious, immediate, and ongoing risk of identity fraud. Additionally, Defendant's failures caused costs and expenses associated with the time spent and the loss of productivity from taking time to address and attempt to ameliorate the release of Private Information, as well as emotional grief associated with constant monitoring of personal banking and credit accounts. Mitigating and dealing with the actual and future consequences of the Data Breach has also created a number of future consequences for Plaintiff and Class members—including, as appropriate, reviewing records of

[2] Defendant posted a form notice on various state attorneys general data breach websites that require entities who have lost consumer or employee information to post a notice if the breach involves one or more of their state's citizens. The Maine Attorney General's data breach page provides an example. *See* Office of the Maine Attorney General, *Snap-On Data Breach Notification*, https://apps.web.maine.gov/online/aeviewer/ME/40/0af7be24-38b6-4a45-92fb-a41e3db04dc2.shtml (last visited June 8, 2022).

[3] Snap-On, *Our Company*, https://www.snapon.com/EN/Our-Company..

fraudulent charges for services billed but not received, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, the loss of property value of their personal information, and the stress, nuisance, and aggravation of dealing with all issues resulting from the Data Breach.

6. The Data Breach was caused and enabled by Defendant's violation of its obligations under statutory and common law to abide by best practices and industry standards concerning the security of employees' records and private information. Defendant failed to comply with security standards and allowed its employees' Private Information to be compromised, which could have been prevented or mitigated after the Data Breach occurred.

7. Accordingly, Plaintiff asserts claims for: negligence; breach of implied contract; unjust enrichment/quasi-contract; breach of fiduciary duty, and state consumer protection statutes, and seeks injunctive relief, monetary damages, statutory damages, as well as all other relief as authorized in equity or by law.

JURISDICTION AND VENUE

8. Snap-On, Inc.'s administrative offices are located at 2801 80th Street, Kenosha, Wisconsin 53143.

9. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. The Court has personal jurisdiction because Defendant's principal place of business is located in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

12. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

PARTIES

A. Plaintiff John Carmack

13. Plaintiff John Carmack is a citizen and resident of Colorado. Plaintiff Carmack was an employee of Snap-On's predecessor, ProQuest, from 1999 through 2006. In 2007, Snap-On acquired ProQuest, and Mr. Carmack continued working for Snap-On for approximately one year. In order to obtain employment at Snap-On, Mr. Carmack was required to provide his Private Information to Defendant. Defendant expressly and impliedly promised to safeguard Carmack's PII. Defendant, however, did not take proper care of employees' PII, leading to its exposure as a direct result of Defendant's inadequate security measures.

14. In or about April of 2022, Plaintiff Carmack received a notification letter from Defendant alerting him to the fact of the Data Breach and that his Private Information was accessed and exfiltrated by cybercriminals, which Private Information included "names, Social Security numbers, date of birth, and employee identification numbers."

15. The letter also offered enrollment of IDX identity protection service, which was and continues to be ineffective for him and Class members. In the months and years following

the Data Breach, Plaintiff Carmack and the Class will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in employee's names without their permission, and targeted advertising without employee consent.

16. Although Plaintiff Carmack is spending time attempting to mitigate the harm done because of the exposure of his Private Information, he is still unsure as to the full extent of the harm.

B. Defendant

17. Defendant, Snap-On, Inc., is a global company headquartered in Wisconsin. Defendant's main location in Kenosha. Defendant manufactures American automotive tools nationwide.[4] Defendant has global reach, with 12,800 employees worldwide, $4.25 billion in 2021, and reach in 130 countries. In the U.S. alone, Snap-On has 3,400 franchise vans and 13 manufacturing facilities. Snap-On's administrative headquarters are located at 2801 80th Street, Kenosha, Wisconsin 53143.

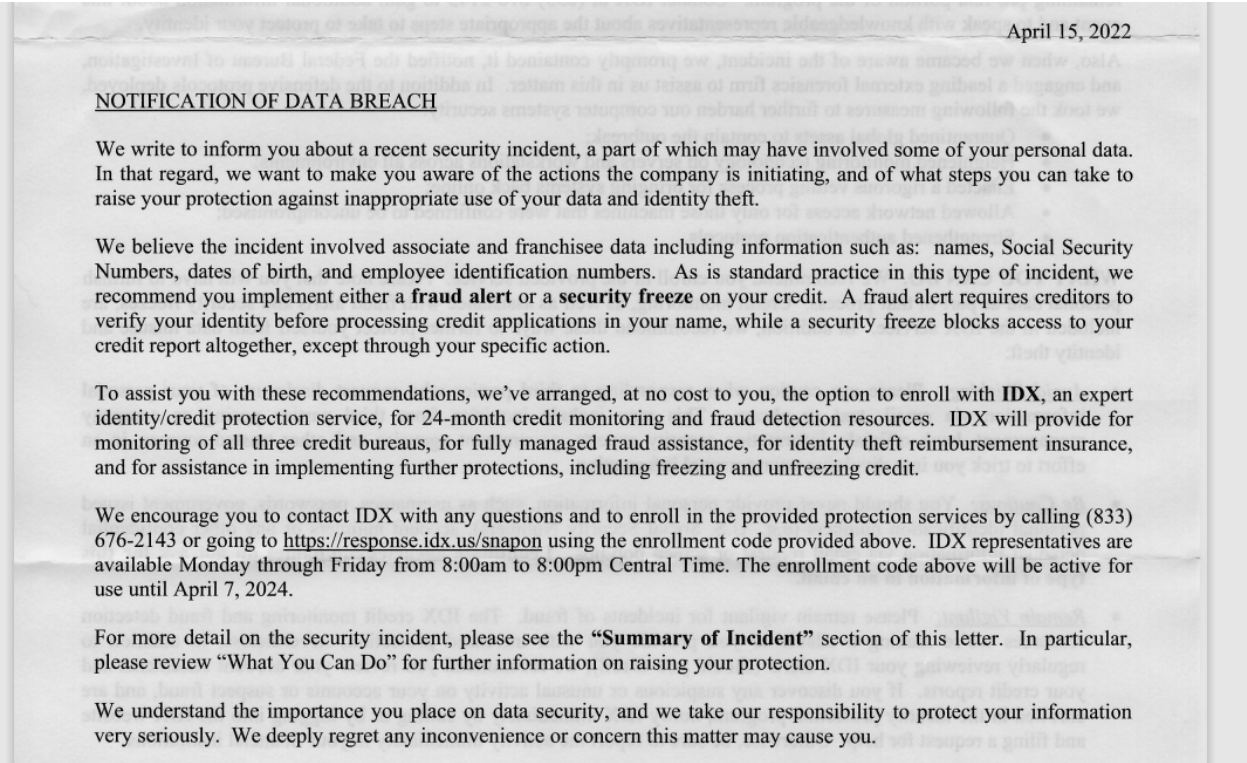
FACTS

18. Snap-On manages 12,800 employees worldwide. As part of its operations, Defendant stores a vast amount of its employees' Private Information. In doing so, Defendant was entrusted with, and obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable laws.

19. In or about April of 2022, Plaintiff Carmack was informed that an unauthorized third party gained access to his former employer's network. Despite sending out notification letters to employees, Defendant has refused to articulate in detail the extent of the information

[4] *Snap-On, Our Company*, https://www.snapon.com/EN/Our-Company..

taken from its systems or how such information may have been used. Snap-On mailed the following notice:



April 15, 2022

NOTIFICATION OF DATA BREACH

We write to inform you about a recent security incident, a part of which may have involved some of your personal data. In that regard, we want to make you aware of the actions the company is initiating, and of what steps you can take to raise your protection against inappropriate use of your data and identity theft.

We believe the incident involved associate and franchisee data including information such as: names, Social Security Numbers, dates of birth, and employee identification numbers. As is standard practice in this type of incident, we recommend you implement either a **fraud alert** or a **security freeze** on your credit. A fraud alert requires creditors to verify your identity before processing credit applications in your name, while a security freeze blocks access to your credit report altogether, except through your specific action.

To assist you with these recommendations, we've arranged, at no cost to you, the option to enroll with **IDX**, an expert identity/credit protection service, for 24-month credit monitoring and fraud detection resources. IDX will provide for monitoring of all three credit bureaus, for fully managed fraud assistance, for identity theft reimbursement insurance, and for assistance in implementing further protections, including freezing and unfreezing credit.

We encourage you to contact IDX with any questions and to enroll in the provided protection services by calling (833) 676-2143 or going to https://response.idx.us/snapon using the enrollment code provided above. IDX representatives are available Monday through Friday from 8:00am to 8:00pm Central Time. The enrollment code above will be active for use until April 7, 2024.

For more detail on the security incident, please see the **"Summary of Incident"** section of this letter. In particular, please review "What You Can Do" for further information on raising your protection.

We understand the importance you place on data security, and we take our responsibility to protect your information very seriously. We deeply regret any inconvenience or concern this matter may cause you.

20. The Data Breach exposed the Private Information of 41,052 individuals' information stored on Defendant's servers.

21. Defendant first notified current and former employees via written letter on or around April 15, 2022—approximately a month and a half after it first identified the Data Breach on March 1-3, 2022. These notice letters stated that files accessed by the unauthorized third party included: "names, Social Security numbers, date of birth, and employee identification numbers."

22. On information and belief, Defendant has yet to affirmatively notify all impacted employees individually regarding what specific kind of data were stolen.

23. The Data Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed

to implement data security measures designed to prevent this attack, despite repeated public warnings to global workplaces about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past. Defendant did not properly contain employee data, which requires a heightened level of protection. Defendant failed to disclose to Plaintiff and Class members the material fact that it did not have adequate data security practices to safeguard employees' personal data, and in fact falsely represented that its security measures were sufficient to protect the Private Information in its possession.

24. Defendant's Press Release notably did not include any information about steps they are taking regarding the obvious threat posed by malevolent actors who stole the Private Information of Plaintiff and the Class members to sell on the black market.

25. Had Plaintiff known that his Private Information would be stored by Snap-On using improper and inadequate security measures, he would have reevaluated what information he chose to provide to Defendant, which collects and stores the data of thousands of employees.

26. Defendant's failure to timely provide formal notice of the Breach to Plaintiff and Class members exacerbated the injuries resulting from the Data Breach.

A. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Employees' Private Information Despite Previous Data Breaches

27. Defendant was aware of or should have been aware of the risk of data breaches for global workplaces, which have had well-publicized breaches from misuse or misconfigurations over recent years.

28. Defendant operates a major global workplace, yet Defendant did not allocate adequate resources for cybersecurity protection of employee information.

29. Defendant's failure to provide adequate security measures to safeguard employees' Private Information is especially egregious because Defendant operates in a field

which has recently been a frequent target of scammers attempting to fraudulently gain access to employees' highly confidential Private Information.

30. Ponemon Institute, an expert in the annual state of cybersecurity, has indicated that 2021 had the highest average cost of data breaches in the past 17 years.[5]

31. In fact, Defendant has been on notice for years that companies are a prime target for scammers because of the amount of confidential employee information maintained. In a study of the manufacturing sector, half of manufacturing companies reported a data breach in 2019 alone.[6]

B. Damages to Plaintiff and the Class

32. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

33. The Private Information obtained by hackers and scammers is an extremely valuable commodity that is commonly traded on the black market and results in the diminishment of the value of a person's electronic presence years into the future when it is misused.

34. Plaintiff and the Class have experienced or currently face a substantial risk of out-of-pocket fraud losses such as loss of funds from bank accounts, fraudulent charges on credit cards, targeted advertising, suspicious phones calls, and similar identity theft.

35. Plaintiff and Class members have also incurred out of pocket costs for protective measures such as credit freezing or payment for phone scam detection.

36. Plaintiff and Class members suffered a loss of the property value of their Private

[5] IBM Security, *Cost of a Breach Data* Report, PONEMON INST. (2021), https://www.ibm.com/security/data-breach.

[6] Arctic Wolf, Top 8 Manufacturing Industry Cyberattacks https://arcticwolf.com/resources/blog/top-8-manufacturing-industry-cyberattacks (citing 2019 Sikich report, https://www.sikich.com/md-report/.)

Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of the loss of the property value of personal information in data breach cases.

37. Members of the Class have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

38. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.

39. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[7]

40. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, loans, or even giving false information to police during an arrest. Private Information can be used to submit false insurance claims, obtain prescription drugs or get medical treatment in the victim's name. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit and tax filings for an indefinite duration.

[7] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id*.

C. The Value of Privacy Protections and Private Information

41. The fact that Plaintiff and Class members' Private Information was stolen—and is likely presently being offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

42. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[8]

43. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[9]

44. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[10]

---

[8] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[9] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, THE WALL STREET JOURNAL (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*] (last visited Oct. 1, 2021).

[10] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

45. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[11] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

46. Employees place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[12]

47. At relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the manufacturing industry.

48. Had Defendant followed industry guidelines by adopting security measures recommended by experts in the field, Defendant would have prevented intrusion into its systems and, ultimately, the theft of its employees' Private Information.

49. Given these facts, any institution that transacts business with employees and then compromises the privacy of employees' Private Information has thus deprived employees of the full monetary value of their transaction.

---

[11] *Web's Hot New Commodity*, *supra* note 10.

[12] *Victims of Identity Theft*, *supra* note 13, at 7.

50. Due to damage from Defendant, Plaintiff and the other Class members now face a greater risk of continuous identity theft.

CLASS ACTION ALLEGATIONS

51. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

52. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23 on behalf of a Nationwide Class defined as:

> All persons whose Private Information was compromised as a result of the data breach discovered in March of 2022.

53. In addition, and/or in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of the following subclass (the "Colorado Subclass"):

> All residents of Colorado whose Private Information was compromised as a result of the data breach(es) discovered in March of 2022.

54. The Nationwide Class and Colorado Subclass are collectively defined herein as the "Class" or the "Classes."

55. Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

56. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

57. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all class members would be impracticable. On information and belief, the Nationwide Class number in the thousands.

58. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

e. Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

g. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;

h. Whether Defendant was unjustly enriched by its actions; and

i. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

59. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

60. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because his interests do not conflict with the interests of the Classes he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and he will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

61. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

62. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims

against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, Plaintiff and the Colorado Subclass)

63. Plaintiff fully incorporates by reference all of the above paragraphs, as though they are fully set forth herein.

64. Upon Defendant accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected.

65. Defendant owed a duty of care not to subject Plaintiff and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

66. Defendant owed numerous duties to Plaintiff and the Class, including the following:

i. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

ii. To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

iii. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

67. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff and Class members' Private Information and misuse the Private Information and intentionally disclose it to others without consent.

68. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the manufacturing industry.

69. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff and Class members' Private Information.

70. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

71. Because Defendant knew that a breach of its systems would damage thousands of its employees, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

72. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations and common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

73. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

74. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

75. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

76. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

i. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

ii. Failing to adequately monitor the security of Defendant's networks and

systems;

iii. Allowing unauthorized access to Class members' Private Information; and

iv. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

77. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiff and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff and Class members' Private Information during the time it was within Defendant's possession or control.

78. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

79. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

80. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

81. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, Plaintiff and the Colorado Subclass)

82. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

83. Defendant, as employer, held the Private Information on behalf of Plaintiff. Holding Plaintiff and Class members' Private Information was part of Defendant's regular business practices, as agreed by the parties. When Plaintiff and Class member's joined Defendant's employment, they agreed to have their Private Information stored in Defendant's network.

84. Plaintiff and Class members entered implied contracts with Defendant in which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. Plaintiff and Class members were required to share Private Information to obtain employment. In entering such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant and its subsidiaries' data security practices complied with relevant laws and regulations and were consistent with industry standards.

85. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant.

86. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the Data Breach within a reasonable time.

87. As a direct and proximate result of Defendant's breaches of the implied contracts between them and Defendant, Plaintiff and Class members sustained actual losses and damages

as described in detail above.

88. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class members.

COUNT III
UNJUST ENRICHMENT/QUASI-CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, Plaintiff and the Colorado Subclass)

89. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

90. Plaintiff and Class members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information, which Private Information has inherent value. In exchange, Plaintiff and Class members should have been entitled to have Defendant protect their Private Information with adequate data security.

91. Defendant knew that Plaintiff and Class members conferred a benefit on Defendant and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff and Class members' Private Information for business purposes.

92. Defendant failed to secure Plaintiff and Class members' Private Information and, therefore, did not fully compensate Plaintiff and Class members for the value that their Private Information provided.

93. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate security practices previously alleged.

94. If Plaintiff and Class members knew that Defendant would not secure their

Private Information using adequate security, they would have made alternative healthcare choices that excluded Defendant.

95. Plaintiff and Class members have no adequate remedy at law.

96. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

97. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, Plaintiff and the Colorado Subclass)

98. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

99. Defendant had a fiduciary duty to safeguard employee Private information, which included Plaintiff and Class members.

100. Defendant breached this duty when it did not protect Plaintiff and Class members' Private Information.

101. Defendant breached this duty when it did not provide adequate and timely notification of the Data Breach to Plaintiff and Class members.

102. Plaintiff and Class members face injuries as a direct and proximate result of Defendant's breaches of its fiduciary duties. These injuries include, but are not limited to:

i. Loss of control over Private information;

ii. Compromise of Private Information;

iii. Lost opportunity costs associated with time spent to protect themselves and mitigate harm;

iv. Continued risk that Plaintiff and Class members Private Information could be stolen again;

v. Future costs associated with time spent protecting themselves from future harm;

vi. Diminished value of Defendant's services;

vii. Diminished value of Private Information;

viii. Anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
VIOLATIONS OF WISCONSIN'S NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION
(Wis. Stat. § 134.98, *et seq*)
(On Behalf of Plaintiff and the Nationwide Class)

103. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

104. Wisconsin's Disposal of records statute reads, in relevant part:

> Notice of unauthorized acquisition of personal information; Wis. Stat. § 134.98
>
> Whenever an entity that collects personal information in the ordinary course of its business becomes aware that an unauthorized person has acquired the personal information, the business shall notify the individuals whose personal information has been acquired.
>
> This law applies to any entity that does business in Wisconsin including a state or local government organization, but does not apply to:
>
> - A business conducted solely by an individual, such as a sole proprietorship

- A federally regulated financial institution, or a person that has a contract with a federally regulated financial institution, if the financial institution has a policy in place to handle the unauthorized acquisition of personal information

- A health care plan, health care clearing house, or a health care provider that transacts personal information electronically, if the plan, clearing house, or provider complies with federal law regulating unauthorized acquisition of personal information
- Personal information under this law means an individual's:
  Name;
  Driver's license or state identification number;
  Financial account number, including credit or debit account number or any security code access code or password that would permit access to an individual's financial account;
  DNA profile; and
  Fingerprint, voice print, retina or iris image, or any other unique physical representation.

105. The fact that an entity has failed to comply with this law may be used as evidence in court to prove that the entity is liable for damages incurred by an individual whose identity has been misappropriated. There are no other penalties imposed by this law.

106. This statue establishes a right to privacy for all individuals who interact with a business, that the entity collected. This creates a duty for manufacturing companies in Wisconsin—like Defendant—to not divulge its employee's sensitive information, and strictly prohibits the sale of such sensitive information.

107. Defendant breached its duties under this statute when the Data Breach divulged Plaintiff and Class members' Private Information to malicious third parties, who then offered this Private Information for sale and, on information and belief, consummated the sale of such Private Information.

108. Plaintiff and Class members have suffered and continue to suffer damages arising from the Data Breach and the sale of their Private Information on the black market. Plaintiff is therefore entitled to the relief under this statute.

COUNT VI
VIOLATIONS OF WISCONSIN'S DECEPTIVE TRADE PRACTICES ACT
(Wis. Stat. § 100.18, *et seq*)
(On Behalf of Plaintiff and the Nationwide Class)

109. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

110. Snap-On is a "person," as defined by Wisc. Stat § 100.18(1).

111. Snap-On advertised, offered, or sold goods or services in Wisconsin and engaged in trade or commerce directly or indirectly affecting the people of Wisconsin, as defined by Wisc. Stat. § 100.18(1).

112. Snap-On engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wisc. Stat. § 100.18, including:

a. By Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the Class's Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' PII, including duties imposed by the FTC Act.

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class members' PII, including by implementing and maintaining reasonable security measures.

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' PII, including duties imposed by the FTC Act.

f. Omitting, suppressing, and concealing the material fact that it did not reasonably of adequately secure Plaintiff and Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with

common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' PII, including duties imposed by the FTC Act.

113. Snap-On's representations and omissions were material because they were likely to deceive reasonable employees about the adequacy of Snap-On's data security and ability to protect the confidentiality of employees' PII.

114. Snap-On acted intentionally, knowingly, and maliciously to violate Wisconsin's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Class members' rights. Numerous past data breaches put it on notice that its security and privacy protections were inadequate

115. Snap-On's conduct is injurious to the public interest because it violates Wisc. Stat. § 100.18, violates a statute that contains a specific legislative declaration of public interest impact, and/or inured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the thousands of Wisconsin residents affected by the data breach.

116. As a direct and proximate result of Snap-On's unfair or deceptive acts or practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII

117. Plaintiff and Class members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties,

and attorneys' fees and costs.

COUNT VII
VIOLATIONS OF THE COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. § 6-1-105, *et seq*
(On behalf of Plaintiff and the Colorado Subclass)

118. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

119. Defendant engaged in transactions an conduct to procure the employment information it obtained on behalf of Plaintiff and the Class.

120. Defendant engaged in trade and commerce through its acts and omissions and its course of business, including obtaining and storing employees' PII, throughout the state of Colorado.

121. Defendant violated Colo. Rev. Stat. § 6-1-105 by engaging in deceptive, unfair, and unlawful trade acts or practices while conducting trade or commerce in Colorado. Defendant's violations include, but are not limited to:

a. Failure to safeguard employee Private Information;

b. Failure to disclose its data security practices were inadequate to protect Plaintiff and Class members' Private Information;

c. Failure to notify Plaintiff and the Class in a timely manner of the Security Breach;

d. Failure to delete, stop accepting, and/or storing employee information after Defendant knew of its inadequate security; and

e. Failure to remediate security issues and harm to Plaintiff and Class members.

122. Plaintiff and Class members are entitled to damages as well as injunctive relief

because Defendant violated the Colorado Deceptive Trade Practices Act.

COUNT VIII
DECLARATORY/INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, Plaintiff and the Colorado Subclass)

123. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

124. This court is authorized under 28 U.S.C. § 2201 *et seq.* to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the state statutes described in this Complaint.

125. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff and Class Members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their PII will occur in the future.

126. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

127. Defendant still possesses the PII of Plaintiff and the Class.

128. Defendant has made no announcement that it has changed its data storage or security practices related to the PII.

129. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

130. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Snap On. The risk of another data breach is real, immediate, and substantial.

131. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Snap-On, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

132. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Snap-On, thus eliminating the additional injuries that would result to Plaintiff and Class Members, along with other consumers whose PII would be further compromised.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully demands a jury trial of all issues so triable and requests that the Court enter judgment in their favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Classes as requested herein, designating Plaintiff as Class Representative, and appointing Class Counsel as requested in Plaintiff's expected motion for class certification;

B. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

C. Ordering injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii)

immediately provide free credit monitoring to all Class members indefinitely;

D. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff and his counsel;

E. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff hereby requests a trial by jury.

Dated this 15th Day of June 2022.

Respectfully submitted,

HAWKS QUINDEL, S.C.,

s/ Larry A. Johnson
Larry A. Johnson SBN:1056619

Hawks Quindel, S.C.
5150 N. Port Washington Rd., Ste. 243
Milwaukee, WI 53217
Telephone: 414-271-8650
Fax: 414-207-6079
E-mail: ljohnson@hq-law.com

Attorneys for Plaintiff (Local Council)

Nicholas A. Migliaccio (pro hac vice forthcoming)
Jason Rathod (pro hac vice forthcoming)
Tyler Bean (pro hac vice forthcoming)
Kevin Leddy (pro hac vice forthcoming)

MIGLIACCIO & RATHOD, LLP
412 H Street NE
Washington, D.C. 20002
202.470.3520
nmigliaccio@classlawdc.com